Exhibit 3

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

PITT MCGEHEE PALMER BONANNI & RIVERS, P.C.
Megan Bonanni*
mbonnani@pittlawpc.com
Kevin M. Carlson*
kcarlson@pittlawpc.com
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
Tel: (248) 398-9800

SOMMERS SCHWARTZ, P.C
Lisa M. Esser*
lesser@sommerspc.com
Jason Thompson*
jthompson@sommerspc.com
Richard L. Groffsky*
rgroffsky@sommerspc.com
Matthew G. Curtis*
mcurtis@sommerspc.com
One Towne Square, 17th Floor
Southfield, MI 48076
Tel: (248) 355-0300

* *denotes PHV forthcoming*

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JANE DOE 1, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

MATTHEW WEISS, CALIFORNIA STATE UNIVERSITY, SAN BERNARDINO, BOARD OF TRUSTEES OF THE CALIFORNIA STATE UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LLC,

Defendants.

Case No.: 5:25-cv-00997

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

ACTION SEEKING STATEWIDE AND NATIONWIDE RELIEF

Plaintiff JANE DOE 1, ("Plaintiff") through her attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Clarkson Law Firm, P.C. for their Complaint against Matthew Weiss, California State University, San Bernardino, and Keffer Development Services, LLC, ("Defendants") states as follows:

I. INTRODUCTION

1. Students and alumni connected to California State University, San Bernardino from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, California State University, San Bernardino and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that California State University, San Bernardino students and student-athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe 1. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

II. PARTIES

Plaintiff:

2. **Plaintiff Jane Doe 1** was a student athlete at California State University, San Bernardino between 2012-2016 and was a member of the Volleyball Team.

3. Plaintiff Jane Doe 1 is domiciled in Orange County, California, in the City of Huntington Beach.

4. On or about March 31, 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Defendants:

5. **California State University, San Bernardino** ("University") is a public university in San Bernardino, State of California, San Bernardino County and is organized and existing under the laws of the State of California. Its principal place of business is in San Bernadino County.

6. University is a part of the California State University system.

7. **The Board of Trustees of the California State University** ("Trustees") oversees the California State University system and is headquartered in Long Beach, California, and The Trustees are therefore sued as a Defendant in this action. (Collectively with California State University, San Bernardino the "University Defendants")

8. **Defendant Keffer Development Services, LLC** ("Keffer") is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systemically conducted business in California by directly providing services to residents and entities within the State of California, thereby availing itself of protections of the law of the State of California.

9. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information ("PII") and personal health information ("PHI") of Plaintiff and Class Members across the country.

10. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

11. **Matthew Weiss** ("Weiss") is an individual residing in the State of Michigan, who had contacts with the State of California in that he conducted illegally activity in the State of California, by hacking into the personal property of Plaintiff and putative Class Members of the State of California during the applicable time

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

period at issue in this Complaint and said activities of which this Complaint arises from.

12. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

III. JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq*.; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq*.; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S. Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

14. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act ("CAFA") as a class action lawsuit in which the amount in controversy exceeds $5,000,000.00, there are more than one-hundred putative Class Members, and a number of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

15. The Court has personal jurisdiction over Defendants named in this action because University Defendants and Trustees are located and created under the laws of the State of California, Defendant Weiss had minimum contacts with the State of California as set forth above, thus purposefully availing himself of the privilege of conducting activities in the State of California. Defendant Keffer directs business at the State of California, conducts substantial business in California, and has availed itself of the protections of California state law. The conduct by Defendant Keffer which gives rise to the claims against Defendant Keffer in this Complaint was directed at and occurred in the State of California.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

16. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to these claims occurred within this District.

17. Plaintiff's injuries are redressable by monetary compensation and injunctive relief, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants' conduct.

IV. COMMON ALLEGATIONS

Weiss' Data Breach and Cyber Sexual Assault of Thousands of Students for Nearly a Decade and the Role Defendant Keffer and University Defendants Played in his Scheme

18. Plaintiff brings this class action against the University Defendants and Keffer for their failure to properly secure the highly sensitive personally identifiable information ("PII") and protected health information ("PHI") of more than 150,000 students, including herself, which was targeted, accessed, and exfiltrated by former University of Michigan and Baltimore Ravens coach and sexual predator Matthew Weiss, over the course of nearly a decade.

19. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to both student databases and student-athlete databases of more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

20. The University Defendants contracted with Defendant Keffer.

21. Due to lack of adequate security measures, failure to monitor their networks, databases, and accounts, Defendants enabled Weiss to gain access to Keffer's and University Defendants' databases, and download highly sensitive PII and PHI of more than 150,000 athletes – including Plaintiff's.

22. Using the information that Weiss obtained from the student-athlete databases, Weiss was then able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

23. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

24. Through this scheme, unknown to students and student athletes, Defendant Weiss downloaded intimate digital photographs and videos of female and male students, and obtained highly sensitive private messages and information about them. Plaintiff was one of these affected students.

25. This scheme appears to be the largest cyber sexual assault of student athletes in U.S. history.

26. The data breach and cyber sexual assault of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for nearly a decade because the University Defendants and Defendant Keffer failed to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

27. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

28. That level of access through that number of accounts is an egregious and grossly negligent failure of data security, as no institution with reasonable data security would allow such a breach over an eight-year period.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

29. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss' perpetration of the cyber sexual assaults and data breach.

Defendant Keffer and its "Athletic Trainer System"

30. Defendant Keffer is a software development vendor that developed an electronic medical record system known as "The Athletic Trainer System," which is used by many schools, colleges, and universities across the United States.[1]

31. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.[2] Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.[3]

32. Upon information and belief, among the universities served by Keffer are Defendant University, Jane Doe 1's alma mater.

33. Keffer represents that its Athletic Trainer System tool was "designed with athletic trainers for athletic trainers," and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.[4]

---

[1] *ATS—Athlete Info*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf (last accessed April 22, 2025).

[2] *Company History*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/CompanyHistory.aspx (last accessed April 22, 2025).

[3] *The Athletic Trainer System*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/Default.aspx (last accessed April 22, 2025).

[4] *See Demo Request or Web Meeting Registration*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/DemoRequest.aspx (last accessed April 22, 2025).

34. In Keffer's FAQ, it boasts that: "Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center" and that "Information security is a high priority in our company."[5] Keffer further claims that "On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance."[6]

35. In Keffer's Privacy Policy, it acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS' legal obligations as a "business associate" under HIPAA."[7]

36. Keffer's Privacy Policy further states: "KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed."[8]

37. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' – including Jane Doe 1's personal identifying information and protected health information.

---

[5] *The Athletic Trainer System FAQ*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf (last accessed April 22, 2025).

[6] *Id.*

[7] *Keffer Development Services, LLC Privacy Policy*, THE ATHLETIC TRAINER SYSTEM (July 2, 2024), https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf (last accessed April 22, 2025).

[8] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

38. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.[9] A two-factor basic security measure, which requires an additional layer of authentication on top of a login credential – such as a code sent via text message or email – would have critically prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

39. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant University's facilities, and thus knowingly and deliberately permitted Plaintiff's confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiff.

40. Recent actions by the FTC underscore the gross negligence and failings of Keffer and the University Defendants in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023, the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[10]

---

[9] *The Athletic Trainer System FAQ*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf (last accessed April 22, 2025).

[10] Alex Gaynor, *Security Principles: Addressing underlying causes of risk in complex systems*, FEDERAL TRADE COMMISSION (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems (last accessed April 22, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

41. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.[11]

42. Keffer and the University Defendants also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiff Jane Doe 1 and those Class Members similarly situated.

43. Both Keffer and the University Defendants had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

44. The risk of identity theft and breaches of security to access users' private, personal, and confidential information is foreseeable within the University Defendants' and Keffer's information technology systems, and the University Defendants and Keffer are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

///

[11] *E.g., In re: Equifax* (July 2019),*Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FEDERAL TRADE COMMISSION (July 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach (last accessed April 22, 2025). ; *In re Drizly* (Oct. 2022), *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers*, FEDERAL TRADE COMMISSION (Oct. 24, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million (last accessed April 22, 2025).

University Defendants' Failure to Safeguard its Students' Private Information for Nearly a Decade

45. California State University-San Bernardino is a high-level educational institution, with a diverse athletic program, enrolling hundreds of student athletes at any one time across over a dozen sports.

46. In maintaining its highly regarded athletics department and programs, California State University-San Bernardino provides its student athletes with athletic trainers.

47. The University Defendants had a responsibility and duty to oversee the University's operations, policies, and procedures, and care for and protect the University's students.

48. The University Defendants were required to ensure that students, such as Jane Doe 1, were not exposed to sexual predators who would invade their privacy.

49. The University Defendants failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe 1 and other Class Members as alleged in this Complaint.

50. This prolific and egregious breach and violation was entirely preventable by the University Defendants and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached Keffer's and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems of Keffer and these universities and colleges and authentication processes. On information and belief, neither the University Defendants nor Keffer required that their employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI ("Protected Health Information").

51. The breach and cyber assaults were a direct result of the University's and Keffer's failure to implement adequate and reasonable cyber-security procedures and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

protocols necessary to protect Jane Doe 1 and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe 1, vulnerable to exploitation by malicious predators like Defendant Weiss.

52. The University Defendants were grossly negligent on two fronts: (1) in their hiring and oversight of Defendant Keffer and their entrusting of students' PII and PHI in the care of Defendant Keffer, and (2) in their maintenance, oversight and security of their own internal databases of those internal systems to protect student PII and PHI.

53. The University Defendants took no reasonable actions to prevent this access despite their duties to students and have taken no reasonable actions to notify or rectify harm to the victims of Matthew Weiss' misconduct and predation.

54. Thousands of students still remain at risk because the University Defendants and Keffer have failed to undertake any reasonable review of how Jane Doe 1's private and personal information is stored, maintained, and who can access such information, and from where.

55. To this day, the University Defendants have not formally informed Class Members impacted by Weiss' cyber sexual assault and misconduct.

University Defendants Were Negligent in Hiring/Contracting with Defendant Keffer and in Entrusting Students PII and PHI to Keffer

56. University Defendants provided its student athletes with medical treatment, including from athletic trainer employees of the University.

57. To facilitate that treatment, the University Defendants contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University Defendants and Keffer with sensitive PII and PHI.

58. When collecting that information, the University, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a "business associate" under HIPAA.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

59. Jane Doe 1 and others similar to her entrusted that the University Defendants and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

60. The University Defendants and Keffer had, and continue to have, a duty to protect Jane Doe 1 and to take appropriate security measures to protect private, personal, medical, and intimate information, communications, and images.

61. The University Defendants knowingly and deliberately permitted access to and the divulging of Plaintiff's stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe 1 and others like her.

62. Upon information and belief, the University Defendants failed to properly investigate Keffer, Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

63. The University Defendants were negligent and/or reckless in failing to ensure that media and other private, personal, and sensitive information, including but not limited to those of Jane Doe 1, were securely protected, as the University Defendants were entrusted to do.

64. The University Defendants failed to implement the security measures necessary to protect their students PII and PHI, including failing to train staff and employees on securing credentials, requiring multi-or-two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University Defendants entrusted students' sensitive PII and PHI and monitoring and auditing access to students' files and private information.

65. In other words, the University Defendants not only failed to ensure they had implemented sufficient security protocols and procedures across their own systems and staff, but also the University Defendants failed to ensure Keffer had

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

adequate security measures in place to protect its students' PII and PHI from theft and misuse.

66. Indeed, the University Defendants lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

67. The University Defendants and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

68. Because Keffer and the University Defendants failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

69. All Defendants disregarded the rights of Jane Doe 1 and Class Members. The University Defendants and Keffer knowingly, intentionally, willfully, recklessly, and/or negligently provided access to and/or divulged Plaintiff's private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train their staff and employees on proper security measures; failed to provide Jane Doe 1 and the Class Members prompt notice of the data breach and cyber assault.

70. Defendants University's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe 1 under common law tort claims and state and federal statutory law, rendering them liable to Jane Doe 1 and the Class Members for

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

the harms caused by this egregious and preventable cyber sexual assault and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe 1 and the Class Members by his intentional hacking and exfiltration of their private information under tort and statutory law.

71. Jane Doe 1 and the punitive Class Members are current and former students at the University and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

72. Jane Doe 1 and the punitive Class Members suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

73. Jane Doe 1 seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

74. Jane Doe 1 seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

Jane Doe 1's Allegations

75. Plaintiff Jane Doe 1 is a former __student at California State University-San Bernardino.

76. While in school at the University, Jane Doe 1 participated in the Volleyball program while Defendant Weiss' data breach and cyber sexual assault was ongoing.

77. As a student athlete, Jane Doe 1 received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 1 was required to use the Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer system.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

78. As a student, Jane Doe 1 was required to disclose personal information to the University and was issued a University email where sensitive, personal information was stored.

79. Because Keffer and the University Defendants never implemented the security safeguards needed to protect Jane Doe 1's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University Defendants and/or Keffer's Athletic Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

80. Defendant Weiss compromised all information that was saved in the University Defendants and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

81. On March 26, 2025, Jane Doe 1 received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss.

82. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"[12] Jane Doe 1 felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy – symptoms that are further exacerbated by the fact that Jane Doe 1 still does not have a full and complete understanding of the data breach and cyber sexual assault enabled by the University Defendants and perpetrated by Defendant Weiss.

83. This cyber sexual assault invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were preventable by University Defendants and Defendant Keffer.

[12] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

84. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

85. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe 1 and those similarly situated have incurred substantial monetary and emotional harm exceeding $5,000,000, exclusive of costs, interest, and fees.

Defendants Keffer and University Defendants Failed to Properly Protect Plaintiff's and Class Members' PII And PHI

86. Defendants Keffer and University Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

87. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

88. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[13]

---

[13] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed April 22, 2025).

The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

89. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

90. Defendants Keffer and the University Defendants failed to properly implement the basic data security practices explained and set forth by the FTC.

91. Defendants Keffer's and University's failure to employ reasonable and appropriate measures to protect against unauthorized access PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. A systematic, years-long breach such as the ones Defendants Keffer and the University Defendants experienced, is also considered a breach under the HIPAA Rules because there is unauthorized access to PHI that is not permitted under HIPAA.

93. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

94. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

///

///

[14] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).[15]

95. Defendants Keffer's and University's data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and the University Defendants failed to comply with safeguards mandated by HIPAA.

University Defendants and Keffer Failed to Comply with Industry Standards

96. Defendants Keffer and the University Defendants did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

97. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[16]

98. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and

---

[15] *FACT SHEET: Ransomware and HIPAA*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed April 22, 2025).

[16] *See Ransomware Prevention and Response for CISOs*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed April 22, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework ("SPF"), Domain Message Authentication Reporting and Conformance ("DMARC"), and DomainKeys Identified Mail ("DKIM") to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

- Implement Software Restriction Policies ("SRP") or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol ("RDP") if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. [17]

99. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems ("Oss") have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in

[17] *Id*. at 3-4.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[18]

100. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and the University

[18] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Sep. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed April 22, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

101. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

102. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and University, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

103. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

104. Given that Defendants Keffer and the University Defendants were storing the private information of 150,000 individuals combined, Defendants Keffer and the University Defendants could and should have implemented all of the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

105. The occurrence, scope, and duration of the breach and cyber sexual assaults indicate that Defendants Keffer and the University Defendants failed to

[19] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (March 5, 2020), https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed April 22, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

Defendants Keffer and the University Defendants Failed to Properly Protect PII and PHI

106. Defendants Keffer and the University Defendants breached their obligations to Jane Doe 1 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
b. Failing to adequately protect students' private information;
c. Failing to properly monitor its own data security systems for existing or prior intrusions;
d. Failing to test and assess the adequacy of its data security system;
e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. §164.304 definition of encryption);

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

q. Failing to adhere to industry standards for cybersecurity.

107. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and the University Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' private, sensitive information.

108. The University Defendants were also grossly negligent in their failure to oversee the data security practices of third-party vendor—Keffer—in which they entrusted the sensitive private information of their students and former students.

109. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

Defendants Caused Plaintiff and the Class Members to Suffer Loss of Privacy and Dignitary Harm

110. Defendants' conduct enabled a significant violation of privacy, extending far beyond the mere loss of data. The type of information compromised ranged from personal information like names, contact information and passwords to medical and psychological information and intimate photos and communications that were never meant for public viewing or viewing by an unauthorized third party. When extremely sensitive personal information such as this is compromised, individuals face a cascade of potential harm that erodes their sense of security and control, as information that they thought would remain confidential and private has now been leaked to the outside world, and which they no longer exercise control over. This exposure can lead to a profound sense of vulnerability, as individuals grapple with the knowledge that their most personal details are now in the hands of unknown actors, free to circulate and be publicized now, or at any time in the future.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

111. Information regarding an individual's health and medical choices, such as here, as well as private communications and intimate photos meant for a romantic partner are among the most sensitive information there is. An individual's right to privacy regarding their body, their medical and psychological care, their romantic interests and their sexual and intimate life are the most sacrosanct and inviolable rights an individual possesses, striking to the very core of their personhood and dignity. Harm relating to an individual's loss of privacy and dignitary harm, especially with information as sensitive as this, has also long been recognized by courts and in the common law.

112. When an individual loses this privacy and such sensitive information is viewed by a third party without their knowledge or consent, this harm cannot be undone. Weiss' unlawful and immoral violation of the personal and intimate lives of thousands of young people shocks the conscience and causes humiliation and loss of dignity that cannot be easily undone. The University Defendants and Keffer's failure to safeguard this sensitive information has stripped Plaintiff and the Class Members of this essential control, exposing them to the potential for enduring emotional distress and the profound sense of vulnerability that accompanies the exposure of deeply private matters.

113. By stripping Plaintiff and the Class Members of their right to control this sensitive information about themselves, Defendants have done immense harm to Plaintiff and the Class Members' rights to privacy as well as their personal dignity and bodily sovereignty. This permanent loss of security and fundamental right to privacy and bodily autonomy is harm that no compensation can ever fully restore.

V. TOLLING

114. Plaintiff realleges and incorporate by reference all preceding allegations as though fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

115. The statutes of limitations applicable to Plaintiff's claims were tolled by Defendants' conduct and Plaintiff's and Class Members delayed discovery of their claims.

116. As alleged above, Plaintiff did not know, and could not have known, that Defendant Weiss would have surreptitiously obtained her personal photographs and information without her consent.

117. The Defendants' alleged unlawful conduct could not have been discovered until at least March 2025 when Plaintiff was notified by the Department of Justice that her information was found in possession of Weiss who obtained it through illegal means.

118. Plaintiff could not have discovered, through the exercise of reasonable diligence, the full scope of Defendants' alleged unlawful conduct, as Weiss surreptitiously accessed her information and the other Defendants failed to stop him or otherwise make Plaintiff and the Class Members aware of this illegal activity.

119. All applicable statutes of limitations have been tolled by operation of the delayed discovery rule. Under the circumstances, Defendants were under a duty to disclose the nature and significance of the invasion of privacy but did not do so. Defendants are therefore estopped from relying on any statute of limitations.

VI. CLASS ALLEGATIONS

120. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

Nationwide Class:

> All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the "Class Members").

121. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

likely violation of their privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows:

California Subclass:

> All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the "DOJ Letter Sub-Class").

122. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge's staff; and (c) the attorneys representing any parties to this Class Action.

123. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

124. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

125. The Fed. R. Civ. P. 23(a) elements of Numerosity, Commonality, Typicality, and Adequacy are all satisfied.

126. **Numerosity:** Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand, satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery and the number is great enough such that joinder is impracticable.

127. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

128. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

129. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the University, and Keffer.

130. Electronic records maintained by the University Defendants and Keffer can confirm the identification of Class Members.

131. **Commonality:** Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense.

132. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff's and Class Members' claims are the same, common to all; as is true of the evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

133. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff's and other Class Members occurred are identical.

134. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

135. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

136. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

(a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;

(b) Whether Defendants Keefer and the University Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;

(c) Whether Defendants Keefer and the University's data security systems prior to and during the data breach and cyber sexual assault complied with applicable data security laws and regulations;

(d) Whether Defendants Keefer's and the University's data security systems prior to and during the data breach and cyber sexual assault were consistent with industry standards;

(e) Whether Defendants Keefer and the University Defendants owed a duty to Plaintiff and Class Members to safeguard their private information;

(f) Whether Defendants Keefer and the University Defendants breached their duty to Plaintiff and Class Members to safeguard their private information;

(g) Whether the University Defendants were grossly negligent and/or negligent in their oversight of Defendant Keffer;

(h) Whether the University Defendants or Keffer knew or should have known that their data security systems and monitoring processes were deficient;

(i) Whether Defendants Keefer and the University Defendants owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber sexual assaults, and whether Defendants

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Keefer and the University Defendants breached that duty to provide timely notice;

(j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

(k) Whether Defendants' conduct was negligent or grossly negligent;

(l) Whether Defendants' conduct was per se negligent;

(m) Whether Defendants' conduct violated federal laws;

(n) Whether Defendants' conduct violated state laws;

(o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and

(p) Other common questions of fact and law relative to this case that remain to be discovered.

137. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

138. Predominance does not require Plaintiff to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D. Ohio 2021) (finding individualized damages questions also do not defeat a predominance finding and noting "when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.") (citing *Hicks v. State Farm Fire & Cas. Co.,* 965 F.3d 460 (6th Cir. 2020).)

139. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants' malfeasance.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

140. Plaintiff's claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiff. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

141. In *Halliburton Co. v. Erica P. John Fund, Inc.,* 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as Plaintiff could show that their evidence is capable of proving the key elements to Plaintiff's claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the Plaintiff did not raise individualized questions sufficient to defeat predominance. "That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate." *Id.*

142. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

143. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de facto* bar to certification. *Nixon,* 2021 WL 4037824, at *8 (citing *Young,* 693 F.3d at 540); *In re Visa Check/MasterMoney Antitrust Litig.,* 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title Ins. Co.,* 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery."); *Slapikas v. First Am. Title Ins. Co.,* 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that "no database exists easily and efficiently to make the determination that would be required for each file").

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

144. Any remaining disputes on membership or class members damages can be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff'd,* 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

145. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

146. **Superiority:** The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

147. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results.

148. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

149. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

150. Pursuing this matter as a class action is superior to individual actions because:

(a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;

(b) Many victims will not come forward without a certified class;

(c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;

(d) This action is manageable as a class action and would be impractical to adjudicate any other way;

(e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,

(f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

151. **Particular Issues:** In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

152. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

///

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT ONE

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030

(*Against Defendant Weiss*)

153. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

154. Plaintiff alleges that Defendant Weiss violated the Computer Fraud and Abuse Act.

155. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

156. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" 18 U.S.C. § 1030(a)(2)(C).

157. Weiss' actions were deliberate because he knew he was unauthorized and proceeded, nevertheless.

158. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

159. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiff and other Class Members, Plaintiff should be awarded all appropriate damages in this matter.

COUNT TWO

VIOLATIONS OF THE STORED COMMUNICATIONS ACT

U.S.C. § 2701 *et seq.*

(*Against Defendants Weiss, Keffer and the University Defendants*)

160. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

161. Plaintiff alleges that Defendants Weiss, Keffer and the University Defendants violated the Stored Communications Act.

162. The Stored Communications Act, 18 U.S.C. § 2701 *et seq*., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by the University Defendants and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiff and others situated similarly to Plaintiff.

163. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

164. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

165. Plaintiff's electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

166. Defendant Weiss was not authorized to access or divulge the content of Plaintiff's private communications for any purpose; and yet, the University Defendants and Keffer enabled Weiss to access Plaintiff's electronic information and communications.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

167. The information, messages, files, and media were accessed by Weiss without authorization.

168. Weiss' access without authorization was deliberate.

169. There is no manner in which Plaintiff's private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had the University Defendants and Keffer not knowingly divulged or permitted access to such information, through Keffer Development other channels, despite knowing that the information would not be protected.

170. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

171. This law imposes strict liability on violators.

172. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than $1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

173. Defendants' access to and divulging of Plaintiff's private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

174. The University Defendants, Kefferand Weiss knew they did not have authority to access and divulge Plaintiff's private, personal, and intimate information, messages, files, and media but did so anyway.

175. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

176. As a result of these violations, Plaintiff has incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiff seeks appropriate compensation for her damages.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

177. Under the statute, Plaintiff should be granted the greater of (1) the sum of her actual damages suffered and any profits made by the University Defendants, Keffer and Weiss as a result of the violations or (2) $1,000 per violation of the Stored Communications Act.

178. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

179. Plaintiff should also be granted reasonable attorney fees and costs.

COUNT THREE

VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) *et seq.*

(*Against Defendants Trustees and the University*)

180. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

181. Plaintiff alleges that the University Defendants violated Title IX, 20 U.S.C. § 1681(A) *et seq*.

182. These Defendants receive federal financial support for their educational programs and are therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq*.

183. Title IX mandates that "No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ..."

184. Each Plaintiff and Class Member is a "person" under the Title IX statutory language.

185. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

186. The University Defendants, under Title IX, are obligated to investigate allegations of sexual harassment.

187. The University Defendants were aware of the sensitive nature of the private and personal information of Plaintiff to which Weiss was able to access.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

188. The University Defendants acted with deliberate indifference to sexual harassment by:

a. Failing to protect Plaintiff and others as required by Title IX;

b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiff provided;

c. Failing to institute corrective measures to prevent Weiss from sexually harassing students; and

d. Failing to adequately investigate the other multiple acts of deliberate indifference.

189. The University Defendants acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

190. The University Defendants' failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

191. At the time the Plaintiff received some medical and/or athletic training services from the University, she did not know the Defendants failed to adequately consider her safety.

192. As a result of the University Defendants' deliberate indifference, Plaintiff have suffered loss of educational opportunities and/or benefits.

193. Plaintiff has incurred, and will continue to incur, attorney's fees and costs of litigation.

194. At the time of the University Defendants' misconduct and wrongful actions and inactions, Plaintiff was unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

195. The University Defendants maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

196. The University Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created an increased risk of sexual harassment.

197. Despite being able to prevent these privacy violations and acts of harassment, the University Defendants failed to do so.

198. Because of the University Defendants' policy and/or practice of deliberate indifference, Plaintiff had her privacy invaded and was sexually harassed by Weiss.

199. Plaintiff should be awarded all such forms of damages in this case for the University Defendants conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT FOUR

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983 - UNREASONABLE SEARCH AND SEIZURE

(*Against Defendant Weiss*)

200. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

201. Plaintiff alleges Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

202. On information and belief, Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this Count, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically her Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

203. At the time of his actions giving rise to this count, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiff's private information without her consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiff's clearly established rights under the Fourth Amendment.

204. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

205. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

206. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function." *Id*. (quoting *Skinner v. Railway Labor Executives' Assn*., 489 U.S. 602, 613-614 (1989)).

207. Plaintiff had a reasonable and legitimate expectation of privacy in her private, personal, and intimate information and images.

208. Acting under color of law, Defendant Weiss violated Plaintiff's clearly established right not to have her private, personal, and intimate information and images accessed, searched, viewed, and seized when he searched and seized Plaintiff's private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiff's reasonable and legitimate expectation of privacy in that information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

209. Defendant Weiss' search and seizure of Plaintiff's personal information was per se unreasonable under the Fourth Amendment.

210. Defendant Weiss' search and seizure of Plaintiff's private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

211. Defendant Weiss is not entitled to qualified immunity because Plaintiff's rights under the Fourth Amendment not to have her personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious and clearly established when Weiss accessed Plaintiff's private information, such that no reasonable person in Weiss' position would believe that the act of searching and seizing Plaintiff's private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiff's rights under the Fourth Amendment. See, e.g., *G.C. v. Owensboro Public Schools*, 711 F.3d 623 (6th Cir. 2013) (Holding that high school officials violated the Fourth Amendment by searching a student's cell phone and reading his text messages); see also *Brannum v. Overton* County School Bd., 516 F.3d 489, 499 (Stating that "Some personal liberties are so fundamental to human dignity as to need no specific explication in our Constitution in order to ensure their protection against government invasion[,]" and holding that school officials violated Fourth Amendment by installing cameras to surreptitiously record students in locker rooms.)

212. As a direct and proximate result of Weiss' violation of Plaintiff's Fourth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

213. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT FIVE

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983 - DUE PROCESS/BODILY INTEGRITY

(*Against Defendant Weiss*)

214. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

215. Plaintiff is alleging Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

216. On information and belief, Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this Count, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically her Fourteenth Amendment equal protection right to be free from sexual harassment in an educational setting, and her Fourteenth Amendment due process right to be free from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.,* 457 U.S. 922, 936 n. 18 (1982)).

217. At the time of the actions giving rise to this Count, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiff's private, personal, and intimate information and images violated Plaintiff's fundamental right of due process. *Doe v. Claiborne Cnty., Tenn. By & Through Claiborne Cnty. Bd. of Educ*., 103 F.3d 495, 506-07 (6th Cir. 1996) (Stating that "the Due Process Clause protects students against abusive governmental power as exercised by a school. To be sure, the magnitude of the liberty deprivation that sexual abuse inflicts upon the victim is an abuse of governmental power of the most fundamental sort; it is an unjustified intrusion that strips the very essence of personhood. If the "right to bodily integrity" means anything, it certainly encompasses the right not to be sexually assaulted under

color of law. This conduct is so contrary to fundamental notions of liberty and so lacking of any redeeming social value, that no rational individual could believe that sexual abuse by a state actor is constitutionally permissible under the Due Process Clause.").

218. On information and belief, at the time of his actions giving rise to this Count, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiff's right of bodily integrity, in violation of the Due Process Clause.

219. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

220. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

221. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT SIX

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.

§ 1983 - EQUAL PROTECTION

(*Against Defendant Weiss*)

222. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

223. Plaintiff is alleging Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

224. Weiss' deliberate and intentional actions in accessing Plaintiff's personal, private, and intimate images and information constituted sexual harassment and abuse

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

because Weiss accessed Plaintiff's highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

225. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiff's personal, private, and intimate images and information violated Plaintiff's rights under the Fourteenth Amendment. *Fitzgerald v. Barnstable Sch. Comm*., 555 U.S. 246, 257-258 (2009); see also *Daniels v. Board of Education*, 805 F.2d 203, 206-07 (6th Cir.1986); Gutzwiller v. Fenik, 860 F.2d 1317, 1325 (6th Cir. 1988); *Kitchen v. Chippewa Valley Sch*., 825 F.2d 1004, 1012 (6th Cir. 1987).

226. On information and belief, at the time of his actions giving rise to this Count, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

227. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

228. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT SEVEN

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY

(*Against Defendant Weiss*)

229. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

230. Plaintiff alleges that Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

231. On information and belief, Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this Count, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically her Fourteenth Amendment due process right to be free of deprivations of property without due process

232. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiff's private, personal, and intimate information and images violated Plaintiff's fundamental right of due process.

233. Plaintiff and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

234. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiff's right not to be deprived of her personal property, in violation of the Due Process Clause.

235. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

236. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

237. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT EIGHT

INVASION OF PRIVACY

(*Against all Defendants*)

238. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

239. Plaintiff and the Class Members had a reasonable and legitimate expectation of privacy in their Private Information that the Defendants failed to adequately protect against compromise from unauthorized third parties.

240. The Defendants owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

241. Defendant Keffer and the University Defendants failed to protect and allowed the Private Information of Plaintiff and Class Members to be exfiltrated and stolen by Defendant Weiss.

242. Defendant Weiss additionally invaded the Privacy of Plaintiff and the Class Members by secretly obtaining their Private Information as well as photos, communications, and other information for his own personal and illicit use without the knowledge or consent of Plaintiff or the Class Members.

243. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendants unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

244. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

245. The University Defendants and Keffer knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

246. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiff and the Class Members undue harm.

247. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, the Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members as other individuals could access Plaintiff's and Class Members highly sensitive communications, messages, photographs, as well as health related information. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the class.

COUNT NINE

INTRUSION UPON SECLUSION

(*Against All Defendants*)

248. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

249. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

250. Plaintiff and Class Members have and had reasonable expectations of privacy in their student records, their provided PII and PHI.

251. The reasonableness of such expectation of privacy is supported by the highly sensitive nature of the records, as well as Defendants' position in power and duty to monitor Plaintiff's and Class Members' collected information.

252. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their Private Information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

253. By failing to keep Plaintiff's and Class Members' Private Information secure, and disclosing Private Information to unauthorized parties for unauthorized use, Defendant Keffer and the University Defendants unlawfully invaded and intruded upon Plaintiff's and Class Members' privacy right to seclusion.

254. Defendant Keffer and the University Defendants' wrongful actions and/or inaction constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their Private Information when they allowed Defendant Weiss to exfiltrate large amounts of Private Information regarding student athletes at the University as well as other institutions.

255. Defendant Weiss also directly invaded the privacy of Plaintiff and the Class Members when he exfiltrated large amounts of data from the computer systems of Keffer and the University Defendants as well as hacking into the personal accounts of thousands of students, student athletes, and alumni.

256. Defendant Weiss' intrusions were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

257. Plaintiff and the Class Members were, and continue to be, harmed as a direct and proximate result of the Defendants' invasion of their privacy by publicly disclosing their Private Information, for which they suffered loss.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

258. As a direct and proximate result of the Defendants' violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT TEN

NEGLIGENCE

(*Against Keffer and the University Defendants*)

259. Plaintiff, individually and on behalf of the Class Members, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

260. The University Defendants and Keffer owed a duty to act with due and reasonable care towards the public and in particular the students of the University as well as other individuals whose information was within Keffer's computer system.

261. The University Defendants and Keffer were aware that its students and their Private Information could be susceptible to unlawful access by third parties.

262. All Defendants owed duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices. Defendants' duties to use reasonable and adequate security measures also arose as a result of the special relationship between Defendants on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted Defendants with their PII/PHI by virtue of their participation in all aspects of school life. Defendants alone could have ensured that their systems, databases, and data storage architecture were sufficient to prevent and minimize the data breach, and yet they failed to do so.

263. Defendants' duties to prevent this data breach, to use reasonable data security measures, and to timely notify students of the affected breach arose under state and federal statutes, which impose on each Defendant mandatory duties to protect and safeguard the PII and PHI of the students' whose information is within their control. These duties are imposed by the Federal Trade Commissions Act, 15 U.S.C. 45, Family Education Rights and Privacy Act ("FERPA"), Student Online

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Personal Information Protection Act, Cal. Bus. & Prof. Code 225841 *et seq.* (Ch. 22.2, Div. 8), California Information Practices Act ("IPA"), Cal. Civ. Code 1798 *et seq.,* Health Information Portability and Accountability Act, and California Confidentiality of Medical Information Act (Cal. Civ. Code 56).

264. None of the Defendants, however, ensured that their computer systems were secure and failed to adequately protect the users of their systems, including students.

265. The University Defendants and Keffer knew the sensitivity of the information kept on its system but failed to ensure that it was secure.

266. For the above reasons and others, the University Defendants and Keffer breached the duty of reasonable care to Plaintiff and the Class Members.

267. Furthermore, University Defendants are also liable for actions of its employees and vendors – including Keffer – under vicarious liability. Each University Defendant had a duty to monitor, supervise, control, and otherwise provide the necessary oversight to safeguard the PII and PHI of their students that they collected, stored, and processed on their and Keffer's systems. At all material times herein, University Defendants had control or the right to control the actions of Keffer, and yet they failed to take any action to ensure that the PII and PHI of their students was protected.

268. As a direct and proximate result of the University Defendants and Keffer's actions and omissions, Plaintiff and the Class Members had their personal information targeted, stolen, and viewed without their knowledge or permission.

269. As a direct and proximate result of the University Defendants and Keffer's general negligence, Plaintiff suffered economic and non-economic damages.

270. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT ELEVEN

STATUTORY CIVIL LARCENY

(*Against Weiss*)

271. Plaintiff, individually and on behalf of the Class Members, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

272. Section 496(a) of the California Penal Code specifically prohibits the obtaining of property "in any manner constituting theft."

273. Section 484 of the California Penal Code defines "theft" to include any actions that "steal, take, carry, lead, or drive away the personal property of another".

274. Plaintiff and the Class Members Private Information, including their personal photos and private communications, were their personal property.

275. Weiss stole, and/or fraudulently appropriated Plaintiff's and the Class Members' personal information without their consent.

276. Plaintiff and the Class Members suffered actual damages as a result of Weiss' theft of their personal property to which he was not entitled.

277. Section 496(c) of the California Penal Code allows any person "injured by a violation" of this section to "bring an action for three times the amount of actual damages, if any, sustained by the Plaintiff, costs of suit, and reasonable attorney's fees."

278. Plaintiff, individually, and on behalf of the Class Members, seeks all monetary and non-monetary relief allowed by law, including treble damages, and attorneys' fees and costs.

COUNT TWELVE

CALIFORNIA INFORMATION PRACTICES ACT, CAL. CIV. CODE § 1798, *et seq.*

(*Against University Defendants*)

279. Plaintiff, individually and on behalf of the Class Members, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

280. The California Information Practices Act ("IPA") requires that agencies report unauthorized disclosure of personal information "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.29.

281. The University Defendants are bound to this duty as they are both an "agency" and more specifically, under Cal. Gov. Code § 1798.3.

282. The Legislature imposed this duty to give notice "in order to protect the privacy of individuals," stating that "is it is necessary that the maintenance and dissemination of personal information be subject to strict limits." Plaintiff and the Class Members suffered the exact harm this statute was meant to avoid, as their "right to privacy is a personal and fundamental right" that was infringed by the University Defendants' negligent notice procedures. Cal. Civ. Code § 1798.1.

283. Plaintiff, individually, on behalf of the Class Members, seeks all monetary and non-monetary relief allowed by law, including treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Proposed Classes defined herein, respectfully request:

A. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding $5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;

B. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;

C. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;

D. Enter judgment in favor of Plaintiff and against Defendant Weiss for treble the amount of their actual damages resulting from Weiss' theft of

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

their personal property, plus attorney's fees and costs for violation of California Penal Code §§ 484 and 496;

E. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and

F. Grant such further relief as is agreeable to equity and good conscience.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all triable issues.

DATED: April 23, 2025

Respectfully Submitted,
CLARKSON LAW FIRM, P.C.

/s/ Yana Hart

Ryan Clarkson, Esq.
Yana Hart, Esq.
Bryan P. Thompson, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

SOMMERS SCHWARTZ, P.C.
Lisa M. Esser (P70628)
Richard L. Groffsky (P32992)
Jason J. Thompson (P47184)
Matthew G. Curtis (P37999)
One Towne Square, 17th Floor
Southfield, MI 48076
Tel: (248) 355-0300

PITT MCGEHEE PALMER BONANNI & RIVERS, P.C.
Megan Bonanni (P52079)
Kevin M. Carlson (P67704)
Beth M. Rivers (P33614)
Danielle Y. Canepa (P82237)
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
Tel: (248) 398-9800

Counsel for Plaintiff and the Proposed Class